HISPOL 011.0

The United States House of Representatives Information Security Policy for Telecommuting

Version:	**2.0**
Approved:	**January 2010**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

This policy provides the House community a secure means for accomplishing work from a remote location. House employees utilize computers when they travel or need to accomplish work remotely after or during normal business hours. A higher level of responsibility for information security lies with remote users since the employee works unobserved, and the work environment falls outside the physical protection of a House facility.

Telecommuting is a working arrangement, mutually agreed upon by the employee and the employing authority, whereby the employee works at an alternative work site on specified days or during specified hours. Such remote users must establish a standard of self-discipline and initiative that ensures secure use of information resources. This means staying up-to-date on all House security policies concerning remote access.

1.1 Scope

The purpose of this document is to provide all users of the House network with guidance governing telecommuting. The scope of this policy includes all House Offices and employees that telecommute to the House.

2 Policy Guidance

2.1 Sensitive Information

It is the responsibility of the employing authority, in conjunction with data owner, to review information sensitivity prior to authorizing employees to conduct House business in a telework arrangement.

All House sensitive information should be marked accordingly. All printed documents and removable media containing sensitive information should be clearly marked "Confidential to the U.S. House of Representatives". Their distribution must be limited to only those House Office staff, employees, contractors, and vendors with a clearly defined need to access the information.

All House sensitive information:

- Must be processed or stored on House owned equipment;
- Must be encrypted[1] when stored on mobile devices; and
- Must not be transmitted on any public access system such as e-mail or via the Internet without protective measures (e.g., using encryption).

[1] Encryption is software or hardware that gives users the capability to convert/recover data that has been put into an unreadable format while it is in transit or in storage. ContactINFOSEC, (202) 226-4988, or the Call Center, (202) 225-6002 / (800) 447-8737, for details.

2.2 Telecommuting User Requirements

The requirements in this section apply to all House telecommuters.

1) SecurID secure two-factor authentication must be used to access the House network. SecurID is the only method supported by the House to access the House network. SecurIDs may be obtained from the Information Systems Security Office (INFOSEC).
2) House information must remain on House equipment at all times.
3) Use only House email accounts to conduct House business and transmit House information.
4) If using personal computer equipment to perform House-related work, use House provided shared resources – not a local computer device – to save information.

2.3 Virtual Private Network (VPN) User Requirements

The House provides a Virtual Private Network (VPN) service for District Offices, telecommuters, and House staff to access the House network via personal computers (PCs) and laptops using high-speed connections, SecurID, and the Internet. Secure use of this service requires that a personal firewall supported by the House VPN solution be installed on the system and operational at the time of each connection to the House network.

2.4 Remote User Requirements

1) Adequate security provisions must be implemented in the remote work environment to protect hardware, software, information, and infrastructure.
2) Special measures must be employed to protect information and access capabilities across dial-up lines, including changing passwords often.
3) Be alert for anomalies and vulnerabilities and report security incidents to INFOSEC.
4) Log off the client device when it is not in use.
5) Access only those House systems that are necessary to perform their job.
6) Establish a thorough understanding and agreement with supervisors regarding appropriate security responsibilities.
7) Avoid uploading and downloading House sensitive information.
8) Encrypt information when it is reasonable and worthwhile.